

DERWENT-ACC-NO: 1996-122409

DERWENT-WEEK: 199613

COPYRIGHT 2004 DERWENT INFORMATION LTD

TITLE: Network system with repeaters and enable-
disable control
circuits set
up corresp. to ports, and similar circuits at
monitoring transmitter, with network administrator
addressed terminals NoAbstract

PATENT-ASSIGNEE: TOSHIBA KK[TOKE]

PRIORITY-DATA: 1994JP-0149722 (June 30, 1994)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE
PAGES MAIN-IPC		
JP 08018582 A	January 19, 1996	N/A
007 H04L 012/40		

APPLICATION-DATA:

PUB-NO	APPL-DESCRIPTOR	APPL-NO
APPL-DATE		
JP 08018582A	N/A	1994JP-0149722
June 30, 1994		

INT-CL (IPC): H04L012/28, H04L012/40 , H04L012/46

ABSTRACTED-PUB-NO:

EQUIVALENT-ABSTRACTS:

TITLE-TERMS: NETWORK SYSTEM REPEATER ENABLE DISABLE CONTROL PORT
RECEIVE ENABLE
DISABLE CIRCUIT SET UP CORRESPOND PORT SIMILAR CIRCUIT
TRANSMIT
NETWORK ADMINISTER MONITOR ADDRESS TERMINAL NOABSTRACT

ADDL-INDEXING-TERMS:

SERVER ROUTER BRIDGE GATEWAY

DERWENT-CLASS: W01

EPI-CODES: W01-A06B1; W01-A06B5A; W01-A06E1; W01-A06G3; W01-A08B1;

SECONDARY-ACC-NO:

Non-CPI Secondary Accession Numbers: N1996-102846

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-18582

(43) 公開日 平成8年(1996)1月19日

(51) Int.Cl.⁶

識別記号

庁内整理番号

F I

技術表示箇所

H 0 4 L 12/40

12/46

12/28

H 0 4 L 11/ 00

3 2 0

3 1 0 C

審査請求 未請求 請求項の数3 O L (全 7 頁)

(21) 出願番号

特願平6-149722

(22) 出願日

平成6年(1994)6月30日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 安東 新

東京都青梅市末広町2丁目9番地 株式会

社東芝青梅工場内

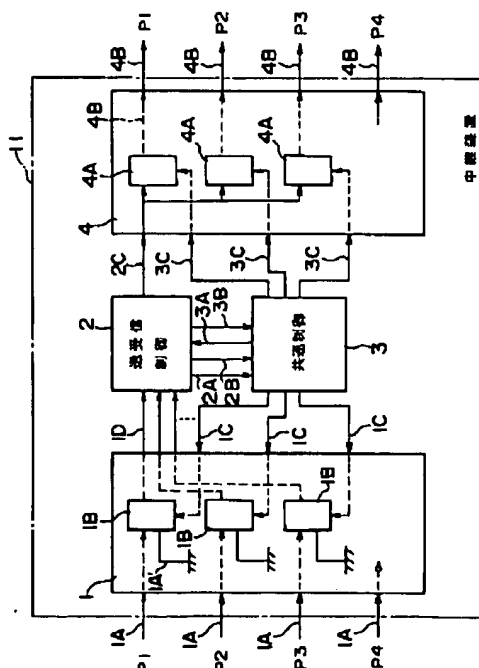
(74) 代理人 弁理士 鈴江 武彦

(54) 【発明の名称】 ネットワーク中継装置およびこれを使用したネットワークシステム

(57) 【要約】

【目的】 各ポートを必要に応じてイネーブル／ディスエーブル制御できるようにして、不正端末によるネットワーク使用の防止を実現する。

【構成】 ネットワーク中継装置11は、ポートP1～P4にそれぞれ対応して設けられた受信イネーブル／ディスエーブル回路1B、および送信イネーブル／ディスエーブル回路4Aを有しており、これら回路は端末からのコマンドによってその送信動作または受信動作がイネーブル／ディスエーブル制御される。このため、例えばネットワークの管理者などが、ネットワーク上の端末アドレスやプロトコルの監視によって不正端末の存在を発見した場合には、その不正端末が存在するネットワークに対応するポートの受信動作などを禁止することができる。



1

【特許請求の範囲】

【請求項1】 ネットワークにそれぞれ接続される複数のポートを有し、それらポート間のデータ転送によってネットワークを相互接続するネットワーク中継装置において、

前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段とを具備することを特徴とするネットワーク中継装置。

【請求項2】 ネットワークにそれぞれ接続される複数のポートを有し、それらポート間のデータ転送によってネットワーク間を相互接続するネットワーク中継装置において、

前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段と、受信動作が禁止されたポートに供給されるデータの送信元アドレスと予め登録された端末のアドレス情報とを比較し、一致した際に該当する送受信装置の受信動作の禁止を解除する受信禁止解除手段とを具備することを特徴とするネットワーク中継装置。

【請求項3】 ネットワーク上の端末から他のネットワーク上の端末へのデータ転送経路が複数設定できるように相互接続された複数のネットワーク中継装置を具備するネットワークシステムであって、

前記各ネットワーク中継装置は、ネットワークに接続される複数のポートと、前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段とを具備し、送信元端末から送信先端末へのデータ転送経路を任意に設定できるようにしたことを特徴とするネットワークシステム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、サーバ、ブリッジ、ルータ、またはゲートウェイ等のネットワーク中継装置、およびそのネットワーク中継装置を使用したネットワークシステムに関する。

【0002】

【従来の技術】一般に、複数のLAN（ローカルエリアネットワーク）やWAN（ワイドエリアネットワーク）を相互に接続する方式として、ブリッジ、ルータ、ゲートウェイ等のネットワーク中継装置が知られている。

【0003】これら各ネットワーク中継装置は、ネットワークセグメントに接続される複数のポートを有しており、それらポート間で受信パケットの転送を行うこと

2

によってネットワークセグメントを相互接続する。ポート間の転送は次のようなフィルタリング処理によって行われる。

【0004】例えば、第1および第2の2つのポートを有するブリッジ装置が第1ポートでパケットを受信した時には、その受信したパケットの宛先アドレスによって指定されるデータステーションが接続されているポートが調べられ、そのポートに受信パケットが転送される。もしそのポートが受信ポートであれば、受信パケットは廃棄される。

【0005】このようなネットワーク中継装置においては、ネットワークシステムの安全性を確保するために、次のようなポート制御が行われている。すなわち、ネットワークに接続されたあるデータステーションが故障し、それがデータ送信し続けことによってネットワーク全体に影響が及ぶことを防止するために、ネットワーク中継装置は、ある一定以上のデータ長を検出した場合、そのポートを論理的に切り離す機能を有している。

【0006】また、信号／衝突検出型のネットワークでは、ある単位時間中に所定回数以上の衝突を検出した場合に、該当するポートを切り離す機能を持つ中継装置もある。

【0007】しかしながら、このような従来のポート制御機能は、ある特定の信号の送受信状態が発生した時に自動的に働くいわゆる障害対策としての機能に過ぎず、正常なプロトコルでデータ送受信が行なわれている限りは何等ポート制御を行うことはできない。

【0008】このため、ネットワーク上に不正端末が存在することが発見された場合であっても、その不正端末が正常な手続きでアクセス動作している限りはポート制御機能は動かない。したがって、不正端末によるネットワークアクセスを防止することはできなかった。

【0009】また、従来のネットワークの形態は、バス、スター、リングの組み合わせでのみ可能であり、一部のネットワークが故障した場合の迂回路形成等が困難であった。

【0010】

【発明が解決しようとする課題】従来のポート制御機能は、ある特定の信号の送受信状態が発生した時に自動的に働くいわゆる障害対策としての機能に過ぎず、正常なプロトコルでデータ送受信が行なわれている限りは何等ポート制御を行うことはできなかった。このため、必要に応じてポートを動的に制御する事ができず、不正端末によるネットワーク使用の防止や、障害発生時の迂回路設定などを行うことができない欠点があった。

【0011】この発明はこの様な点に鑑みてなされたもので、各ポートを必要に応じてイーネブル／ディスエーブル制御できるようにして、不正端末によるネットワーク使用の防止や、障害発生時の迂回路設定などを行うことができるネットワーク中継装置を提供することを目的

とする。

【0012】

【課題を解決するための手段および作用】この発明は、ネットワークにそれぞれ接続される複数のポートを有し、それらポート間のデータ転送によってネットワークを相互接続するネットワーク中継装置において、前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段とを具備することを特徴とする。

【0013】このネットワーク中継装置においては、外部からのコマンドによって任意のポートの送信動作または受信動作をイネーブル／ディスエーブル制御することができる。このため、例えばネットワークの管理者などが、ネットワーク上の端末アドレスやプロトコルの監視によって不正端末の存在を発見した場合には、その不正端末が存在するネットワークに対応するポートの受信動作などをコマンドによって禁止することができる。

【0014】また、この発明は、ネットワークにそれぞれ接続される複数のポートを有し、それらポート間のデータ転送によってネットワーク間を相互接続するネットワーク中継装置において、前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段と、受信動作が禁止されたポートに供給されるデータの送信元アドレスと予め登録された端末のアドレス情報とを比較し、一致した際に該当する送受信装置の受信動作の禁止を解除する受信禁止解除手段とを具備することを特徴とする。

【0015】このネットワーク中継装置においては、受信動作が禁止されたポートに供給されるデータの送信元アドレスが予め登録されたアドレス情報と一致する場合には受信動作が許可されるように構成されており、不正端末以外の他の端末の送受信に影響を与えることなく、不正端末のネットワークアクセスだけを防止することができる。

【0016】また、この発明は、ネットワーク上の端末から他のネットワーク上の端末へのデータ転送経路が複数設定できるように相互接続された複数のネットワーク中継装置を具備するネットワークシステムであって、前記各ネットワーク中継装置は、ネットワークに接続される複数のポートと、前記ポート毎に設けられた複数の送受信装置と、外部からのコマンドを受信し、そのコマンドに応じて前記複数の送受信装置の送信または受信動作をポート毎に個別に許可／禁止するポート制御手段とを具備し、送信元端末から送信先端末へのデータ転送経路を任意に設定できるようにしたことを特徴とする。

【0017】このネットワークシステムにおいては、複

数のネットワーク中継装置を例えばメッシュ状に結合することにより複数のデータ転送経路が設けられており、通常は、ある端末間の経路がポイントツーポイントとなるようにポートのイネーブル／ディスエーブル制御を行っておき、障害発生やトラフィック状態に応じてその経路を動的に変更するといった運用が可能になる。

【0018】

【実施例】以下、図面を参照してこの発明の実施例を説明する。図1にはこの発明の一実施例に係わるネットワーク中継装置を用いたネットワークシステムの構成が示されている。ネットワーク中継装置11は2以上のポートを持つマルチポートタイプの中継装置であり、ここでは、ネットワーク中継装置11が図示のように4つのポートP1～P4を持ち、それらポートP1～P4がそれぞれLANセグメント12～15に接続されている場合を例示して説明する。

【0019】LANセグメント12～15の各々には、データ処理端末が接続されている。これらデータ処理端末は、ワークステーションやパーソナルコンピュータ、またはミニコンピュータ等によって実現されるものであり、対応するLANセグメントを介して相互に通信を行うと共に、ネットワーク中継装置11を介して他のLANセグメント上のデータ処理端末などと通信を行う。

【0020】ネットワーク中継装置11は、例えば、ネットワークサーバ、リピータ、ブリッジ、ルータ、またはゲートウェイ等を構成するものであり、LANセグメント12～15間の相互接続、またはWAN、公衆回線網等に接続するため等に使用される。

【0021】このネットワーク中継装置11は、ポートP1～P4を個別にイネーブル／ディスエーブル制御するためのポートイネーブル／ディスエーブル制御ユニット111を備えている。ポートイネーブル／ディスエーブル制御ユニット111は、斜線で図示されているLANセグメント上の遠隔端末や、またはネットワーク中継装置11に直接接続された管理装置などからの要求に応じて、4つのポートP1～P4それぞれの受信動作および送信動作を個別に制御する事ができる。

【0022】次に、図2を参照して、ネットワーク中継装置11の具体的な構成の一例を説明する。ネットワーク中継装置11は、図示のように、受信部1、送受信制御部2、共通制御部3、および送信部4を備えている。

【0023】受信部1はポートP1～P4それぞれからのパケット受信データ1Aを受信するためのものであり、ポートP1～P4にそれぞれ対応して設けられた4つの受信データイネーブル／ディスエーブル回路1Bを有している。

【0024】これら4つの受信データイネーブル／ディスエーブル回路1Bは、それぞれ対応するポートP1～P4からパケットデータ1Aを受信する回路であり、イネーブル／ディスエーブル信号1Cによってその受信動

5

作が個別に許可/禁止されるように構成されている。

【0025】すなわち、受信データイネーブル/ディスエーブル回路1Bはイネーブルの時には受信データ1Aを選択し、ディスエーブルの場合には接地電位1A⁻を選択する。これら4つの受信データイネーブル/ディスエーブル回路1Bからの受信データ出力1Dは、送受信制御部2に共通に供給される。

【0026】送信部4は、ポートP1~P4それぞれからパケットデータ4Bを送信するためのものであり、ポートP1~P4にそれぞれ対応して設けられた4つの送信データイネーブル/ディスエーブル回路4Aを有している。これら4つの送信データイネーブル/ディスエーブル回路4Aは、それぞれ対応するポートP1~P4からパケットデータ4Bを送信するために設けられた回路であり、イネーブル/ディスエーブル信号3Cによってその受信動作が個別に許可/禁止されるように構成されている。

【0027】4つの送信データイネーブル/ディスエーブル回路4Aには、送受信制御部2からの送信データが共通に供給され、相手先端末に対応するポートに対応する送信データイネーブル/ディスエーブル回路4Aから出力される。

【0028】送受信制御部2は、受信データイネーブル/ディスエーブル回路1Bから受信した受信データの制御、および送信データイネーブル/ディスエーブル回路4Aに出力する送信データの制御を行うためのものであり、通常、クロックリカバリ回路、FIFOバッファ、メモリなどから構成される。また、送受信制御部2は、受信データイネーブル/ディスエーブル回路1Bの制御のために、受信データ2A、および受信クロック2Bを利用して、共通制御3に受信したコマンドなどを送信する。

【0029】共通制御部3は、受信データイネーブル/ディスエーブル回路1B、および送信データイネーブル/ディスエーブル回路4Aをイネーブル/ディスエーブル制御するためのものであり、送受信制御部2から転送されるコマンドに応じて動作する。

【0030】この共通制御部3は、通常、シリアルコントローラ、データシリアル/パラレル変換回路、CPU、メモリなどから構成される。また、34A、3Bは共通制御部3が送受信制御部2との通信にしようとするデータ、クロックなどである。

【0031】次に、図2の中継装置11の動作を説明する。通常、データ転送時には、各ポートの受信イネーブル/ディスエーブル回路1Bは制御信号1Cによって受信データ1Aを選択するイネーブル状態に設定されている。また、各ポートの送信イネーブル/ディスエーブル回路4Aも制御信号3Cにより送信イネーブル状態に設定されている。

【0032】ここで、ネットワークの管理者などが別途

6

ネットワークに接続された装置、または中継装置11の持つ機能などによって、ネットワーク上に不正端末の存在を発見した場合、または障害/トラフィックに応じてあるポートのイネーブル/ディスエーブル制御により経路を変更したい場合を考える。

【0033】この場合、ネットワーク管理者は、ネットワーク13上の所定の端末などを利用して、中継装置11に対してコマンドを発行し、イネーブル/ディスエーブルするポート番号などを通知する。

【0034】この時、ポートP2から受信した中継装置11宛のコマンドは送受信制御部2を経由して共通制御部3に入力される。共通制御部3は、受信コマンドを解析し、それが上記コマンドであった場合には、受信制御信号1Cまたは送信制御信号3C、あるいはそれら両方の制御信号を用いて、送受信のイネーブル/ディスエーブル制御を行う。

【0035】コマンドによってポートP1の受信動作をディスエーブルすることが指定されると、受信部1においては、制御信号1Cにより受信イネーブル/ディスエーブル回路1Bの入力を受信データ1Aから1A⁻に切り替えられ、その受信動作が禁止される。

【0036】この構成においては、端末からコマンドなどによって任意のポートの送信動作または受信動作をイネーブル/ディスエーブル制御することができる。このため、例えばネットワークの管理者などが、ネットワーク上の端末アドレスやプロトコルの監視によって不正端末の存在を発見した場合には、その不正端末が存在するネットワークに対応するポートの受信動作などを禁止することができ、ネットワークの信頼性の向上を図る事ができる。

【0037】次に、図3を参照して、受信イネーブル/ディスエーブル回路1B周辺の他の回路構成を説明する。すなわち、この図3においては、図2の構成に加え、各ポート毎にシリアル/パラレル変換回路1E、パラメータレジスタ1F、および復旧回路1Iを備えている。

【0038】シリアル/パラレル変換回路1Eは、受信イネーブル/ディスエーブル回路1Bと並列に設けられており、受信イネーブル/ディスエーブル回路1Bのイネーブル/ディスエーブル状態に関係なく受信データ1Aを受信し、それをシリアルデータからパラレルデータに変換し、パラメータレジスタ1Fの設定値と比較する。この比較動作は、受信データの送信元アドレスが、パラメータレジスタ1Fに予め設定された受信許可端末のアドレスと一致するか否かを検出するために行われる。

【0039】復旧回路1Iは、制御信号1Cにより受信ディスエーブルが宣告されていても、シリアル/パラレル変換回路1Eから一致検出信号1Hが発生された時には受信イネーブル/ディスエーブル回路1Bをイネーブル

ル状態に設定する回路である。

【0040】すなわち、この図3の構成においては、例えばポートP1が受信ディスエーブルの場合においては、制御信号1C（図3では1J）により受信データ1Aは無視され、1Dには受信データは出力されない。しかし、この状態に於いても、受信データ1Aは常にシリアル/パラレル変換回路1Eにて受信されており、その送信元アドレス（または、送信先アドレスなど）のモニタが行われている。予め登録された各端末の物理アドレスはレジスタ1Fに設定されており、シリアル/パラレル変換回路1Eのアドレス値と常に比較される。

【0041】両者が合致した場合には、信号1Hにてアドレスの一致が復旧回路1Iに通知され、仮に共通制御部3から受信ディスエーブル信号1C（ここでは、1C2）が発生されていても、復旧回路1Iは正当な端末からのデータであると判断し、受信イネーブル/ディスエーブル回路1Bをイネーブル状態に切り替える。

【0042】この場合、受信イネーブル/ディスエーブル回路1Bの受信データの先頭がカットされる危険があるので、ディスエーブル状態であっても受信データを保持するバッファを受信イネーブル/ディスエーブル回路1Bに設けるなどの手法を採用する事が好ましい。この場合、その受信バッファの内容はポートがイネーブルであれば読み出され、ディスエーブルであれば読み出されない。

【0043】この構成においては、受信動作が禁止されたポートに供給されるデータの送信元アドレスが予め登録されたアドレス情報と一致する場合には受信動作が許可されるように構成されているので、不正端末以外の他の端末の送受信に影響を与えることなく、不正端末のネットワークアクセスだけを防止することができる。

【0044】次に、図4を参照して、図2または図3の構成を持つネットワーク中継装置11を用いたネットワークシステムの構築例を説明する。このネットワークシステムにおいては、複数のネットワーク中継装置11が

LANセグメントを介してメッシュ状に結合されており、これによって、あるLANセグメント上の端末から他のLANセグメント上の端末までのデータ転送経路が複数設定されるようになっている。

【0045】この場合、通常は、ある端末間の経路がポイントツーポイントとなるようにポートのイネーブル/ディスエーブル制御を行っており、障害発生やトラフィック状態に応じて、コマンドによるポートのイネーブル/ディスエーブル制御を行ってその経路を自動的または人為的に変更するといった運用を行うことが可能になる。

【0046】

【発明の効果】以上のように、この発明によれば、各ポートを必要に応じてイネーブル/ディスエーブル制御できるようになり、不正端末によるネットワーク使用の防止や、障害発生時の迂回路設定などを行うことが可能となる。

【図面の簡単な説明】

【図1】この発明の一実施例に係わるネットワーク中継装置を用いたネットワークシステムの構成を示すブロック図。

【図2】図1に示したネットワーク中継装置の具体的構成の一例を示すブロック図。

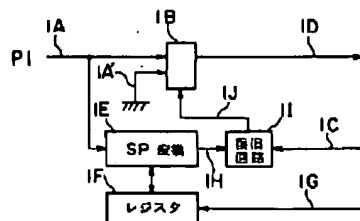
【図3】図1に示したネットワーク中継装置の他の具体的構成の一例を示すブロック図。

【図4】図1のネットワーク中継装置を多数用いて構成したネットワークシステムの一例を示す図。

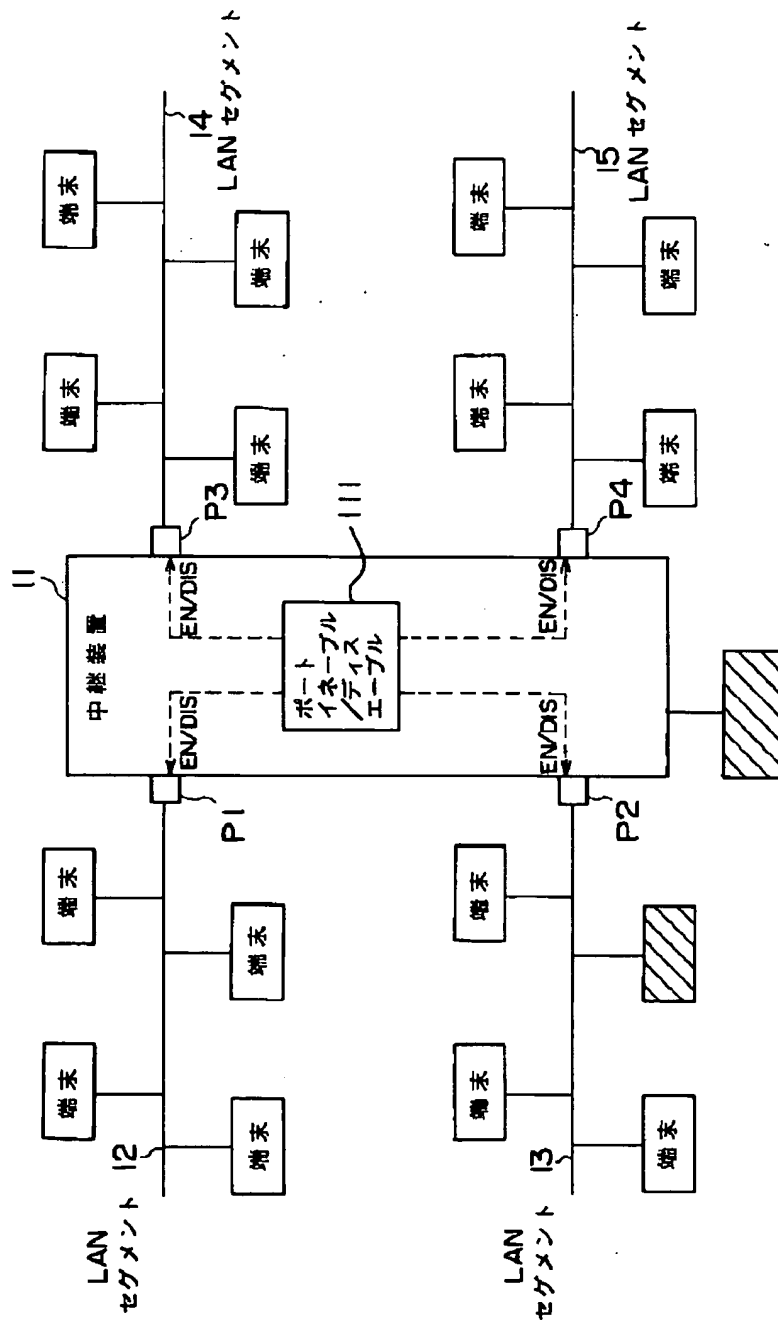
【符号の説明】

1…受信部、1B…受信イネーブル/ディスエーブル回路、1E…シリアル/パラレル変換回路、1F…パラメータレジスタ、1I…復旧回路、2…送受信制御部、3…共通制御部、4…受信部、4A…送信イネーブル/ディスエーブル回路、11…ネットワーク中継装置、12、13、14、15…LANセグメント、P1、P2、P3、P4…ポート。

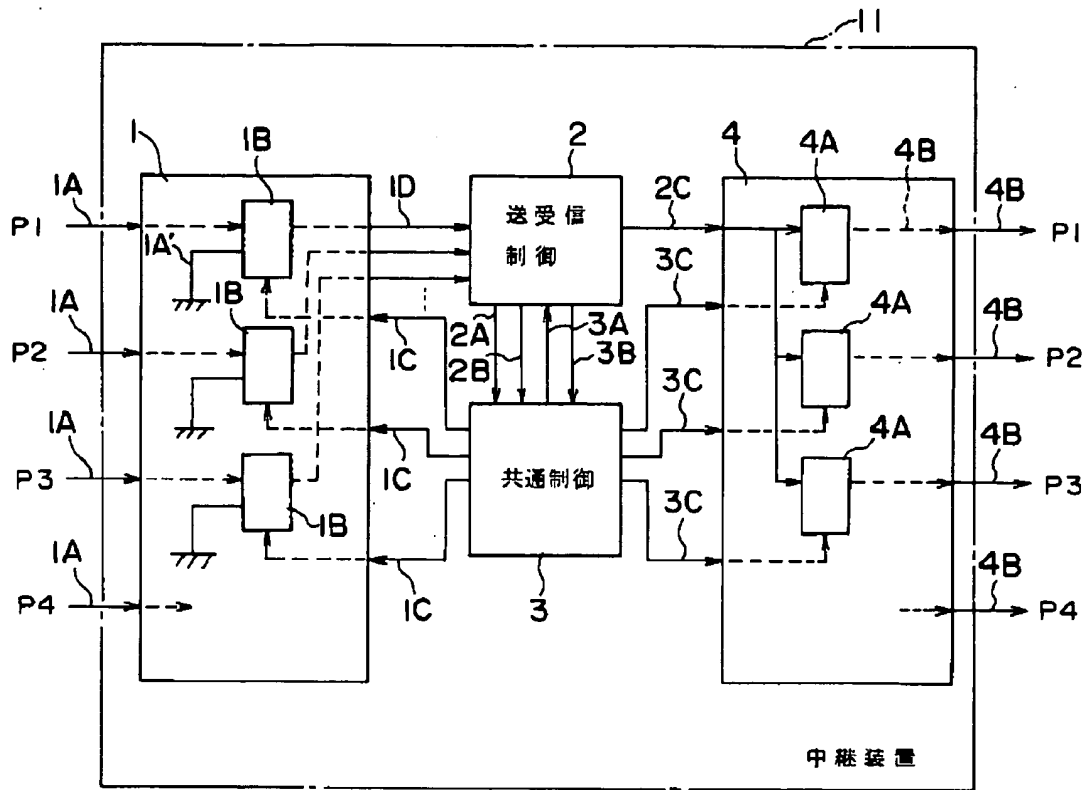
【図3】



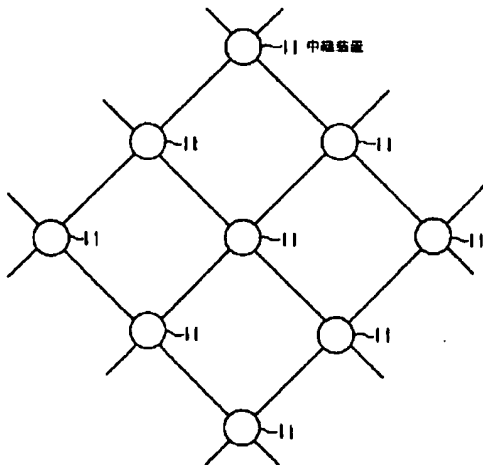
【図1】



【図2】



【図4】



* NOTICES *

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Industrial Application] This invention relates to network repeating installation, such as a server, a bridge, a router, or the gateway, and the network system which used that network repeating installation.

[0002]

[Description of the Prior Art] Generally, network repeating installation, such as a bridge, a router, and the gateway, is known as a method which connects two or more LANs (Local Area Network) and WAN (Wide Area Network) mutually.

[0003] Each [these] network repeating installation has two or more ports connected to a network segment, and interconnects a network segment by transmitting a receive packet among these ports. The transfer between ports is performed by the following filtering processings.

[0004] For example, when the bridge equipment which has two ports, the 1st and the 2nd, receives a packet in the 1st port, the port where the data station specified by the destination address of the packet which received is connected is investigated, and a receive packet is transmitted to the port. A receive packet will be discarded if the port is a receive port.

[0005] In such network repeating installation, in order to secure the safety of a network system, the following port control is performed. That is, a certain data station connected to the network breaks down, and in order to prevent that it continues carrying out data transmission and effect reaches the whole network by things, network repeating installation has the function which separates the port logically, when a certain data length more than fixed is detected.

[0006] Moreover, in the network of a signal / collision-detection mold, when the collision more than the count of predetermined is detected in a certain unit time amount, there is also repeating installation with the function which separates the corresponding port.

[0007] However, such a conventional port control function cannot perform port control at all, as long as it does not pass to the function as the so-called cure against a failure which works automatically but data transmission and reception are performed by the normal protocol, when the transceiver condition of a certain specific signal occurs.

[0008] For this reason, even if that an unjust terminal exists on a network is the case where it is discovered, as long as that unjust terminal is carrying out access actuation in a normal procedure, a port control function is not committed. Therefore, network access by the unjust terminal was not able to be prevented.

[0009] Moreover, the gestalt of the conventional network was possible only in the combination of a bus, a star, and a ring, and detour formation when some networks break down etc. was difficult for it.

[0010]

[Problem(s) to be Solved by the Invention] The conventional port control function was not able to perform port control at all, as long as it did not pass to the function as the so-called cure against a failure which works automatically but data transmission and reception were performed by the normal protocol, when the transceiver condition of a certain specific signal occurred. For this reason, a port could not be

controlled dynamically if needed but there was a fault which can perform neither prevention of the network use by the unjust terminal nor a detour setup at the time of failure generating.

[0011] As this invention was made in view of such a point and can carry out enabling / disable control of each port if needed, it aims at offering the network repeating installation which can perform prevention of the network use by the unjust terminal, a detour setup at the time of failure generating, etc.

[0012]

[Means for Solving the Problem and its Function] This invention is characterized by to provide the port control means which has two or more ports connected to a network, respectively, receives two or more transmitter-receivers prepared for said every port, and the command from the outside, responds to that command in the network repeating installation which interconnects a network by the data transfer between these ports, and permits / forbids transmission or reception actuation of two or more of said transmitter-receivers according to an individual for every port.

[0013] In this network repeating installation, the send action of the port of arbitration or reception actuation enables/is [disable] controllable with the command from the outside. for this reason -- for example, when a network manager etc. discovers existence of an unjust terminal by the monitor of the terminal address on a network, or a protocol, reception actuation of the port corresponding to the network where that unjust terminal exists etc. can be forbidden with a command.

[0014] Moreover, this invention has two or more ports connected to a network, respectively, and sets them to the network repeating installation which interconnects between networks by the data transfer between these ports. Two or more transmitter-receivers prepared for said every port, and the port control means which receives the command from the outside, responds to the command, and permits / forbids transmission or reception actuation of two or more of said transmitter-receivers according to an individual for every port, It is characterized by providing a reception prohibition discharge means to cancel prohibition of reception actuation of the transmitter-receiver which compares the transmitting agency address of the data supplied to the port where reception actuation was forbidden with the address information of the terminal registered beforehand, and corresponds when in agreement.

[0015] Only network access of an unjust terminal can be prevented in this network repeating installation, without being constituted so that reception actuation may be permitted and affecting transmission and reception of other terminals other than an unjust terminal, in being in agreement with the address information into which the transmitting agency address of the data supplied to the port where reception actuation was forbidden was registered beforehand.

[0016] Moreover, this invention is a network system possessing two or more network repeating installation which interconnected so that the multi-statement of the data transfer path to the terminal [terminal / on a network] on other networks could be carried out. Two or more ports where said each network repeating installation is connected to a network, Two or more transmitter-receivers prepared for said every port and the command from the outside are received. The port control means which responds to the command, and permits / forbids transmission or reception actuation of two or more of said transmitter-receivers according to an individual for every port is provided, and it is characterized by enabling it to set the data transfer path from a transmitting agency terminal to the end of a transmitting tip as arbitration.

[0017] In this network system, by combining two or more network repeating installation for example, in the shape of a mesh, two or more data transfer paths are established, enabling / disable control of a port are usually performed so that the path between a certain terminals may serve as a point-to-point, and employment of changing that path dynamically according to failure generating or a traffic condition is attained.

[0018]

[Example] Hereafter, the example of this invention is explained with reference to a drawing. The configuration of the network system using the network repeating installation concerning one example of this invention is shown in drawing 1 . It is multiport type repeating installation with two or more ports, and the network repeating installation 11 has four ports P1-P4 like illustration, and the network

repeating installation 11 illustrates the case where these ports P1-P4 are connected to the LAN segments 12-15, respectively, and explains them here.

[0019] The data-processing terminal is connected to each of the LAN segments 12-15. A workstation, a personal computer or a minicomputer, etc. realizes, and these data-processing terminal performs a communication link with the data-processing terminal on other LAN segments etc. through the network repeating installation 11 while communicating mutually through a corresponding LAN segment.

[0020] The network repeating installation 11 constitutes a Network Server, a repeater, a bridge, a router, or the gateway, and it is used in order to connect with the interconnect between the LAN segments 12-15 or WAN, a public line network, etc.

[0021] This network repeating installation 11 is equipped with port enabling / disable control unit 111 for enabling/disable controlling ports P1-P4 according to an individual. the remote terminal on LAN SEGUMEN by which port enabling / disable control unit 111 is illustrated with the slash -- or the demand from management equipment etc. by which direct continuation was carried out to the network repeating installation 11 -- responding -- four ports P1-P4 -- each reception actuation and send action are controllable according to an individual.

[0022] Next, with reference to drawing 2, an example of the concrete configuration of the network repeating installation 11 is explained. The network repeating installation 11 is equipped with a receive section 1, the transmit/receive control section 2, the common control section 3, and the transmitting section 4 like illustration.

[0023] a receive section 1 -- ports P1-P4 -- respectively -- since -- it is for receiving packet received-data 1A, and has four received-data enabling / disable circuit 1B prepared respectively corresponding to ports P1-P4.

[0024] These four received-data enabling / disable circuit 1B is circuits which receive packet data 1A from the ports P1-P4 which correspond, respectively, and it is constituted so that the reception actuation may be permitted / forbidden by enabling / disable signal 1C according to an individual.

[0025] That is, received-data enabling / disable circuit 1B chooses received-data 1A at the time of enabling, and, in the case of a disable, chooses touch-down potential 1A'. Received-data output 1D from received-data enabling / these four disable circuits 1B is supplied common to the transmit/receive control section 2.

[0026] the transmitting section 4 -- ports P1-P4 -- respectively -- since -- it is for transmitting packet data 4B, and has four transmit data enabling / disable circuit 4A prepared respectively corresponding to ports P1-P4. These four transmit data enabling / disable circuit 4A is the circuits prepared in order to transmit packet data 4B from the ports P1-P4 which correspond, respectively, and it is constituted so that the reception actuation may be permitted / forbidden by enabling / disable signal 3C according to an individual.

[0027] The transmit data from the transmit/receive control section 2 is supplied to transmit data enabling / four disable circuits 4A in common, and is outputted to it from transmit data enabling / disable circuit 4A corresponding to the port corresponding to a phase hand terminal.

[0028] The transmit/receive control section 2 is for controlling the transmit data outputted to transmit data enabling / control-received data received from received-data enabling / disable circuit 1B, and disable circuit 4A, and usually consists of a clock recovery circuit, a FIFO buffer, memory, etc.

Moreover, the transmit/receive control section 2 transmits the command received to common control 3 using received-data 2A and receive-clock 2B for control of received-data enabling / disable circuit 1B.

[0029] The common control section 3 is for enabling/disable controlling received-data enabling / disable circuit 1B, and transmit data enabling / disable circuit 4A, and operates according to the command transmitted from the transmit/receive control section 2.

[0030] This common control section 3 usually consists of a serial controller and data serial/parallel-conversion circuit, a CPU, memory, etc. Moreover, 34A and 3B are data, clocks, etc. which the common control section 3 will make the communication link with the transmit/receive control section 2 and to carry out.

[0031] Next, actuation of the repeating installation 11 of drawing 2 is explained. Reception enabling /

disable circuit 1B of each port are set as the enabling state which chooses received-data 1A by control signal 1C at the time of the usual data transfer. Moreover, transmitting enabling / disable circuit 4A of each port are also set as transmitting enabling state by control signal 3C.

[0032] Here, when a network manager etc. discovers existence of an unjust terminal on a network by the function which the equipment separately connected to the network or repeating installation 11 has, the case where he wants to change a path by enabling / disable control of a certain port according to a failure/traffic is considered.

[0033] In this case, using the predetermined terminal on a network 13 etc., a network administrator publishes a command to repeating installation 11, and notifies enabling / port number which carries out a disable.

[0034] At this time, the received command addressed to repeating-installation 11 is inputted into the common control section 3 via the transmit/receive control section 2 from a port P2. The common control section 3 analyzes a receiving command, and when it is the above-mentioned command, it performs enabling / disable control of transmission and reception using reception-control signal 1C, transmission-control signal 3C, or the control signal of both them.

[0035] If carrying out the disable of the reception actuation of a port P1 with a command is specified, in a receive section 1, control signal 1C will change the input of reception enabling / disable circuit 1B from received-data 1A to 1A', and the reception actuation will be forbidden.

[0036] In this configuration, the send action of the port of arbitration or reception actuation enables/is [disable] controllable from a terminal with a command etc. for this reason -- for example, when a network manager etc. discovers existence of an unjust terminal by the monitor of the terminal address on a network, or a protocol, reception actuation of the port corresponding to the network where that unjust terminal exists etc. can be forbidden, and improvement in network dependability can be aimed at.

[0037] Next, with reference to drawing 3, other circuitry of the reception enabling / disable circuit 1B circumference is explained. Namely, in addition to the configuration of drawing 2, in this drawing 3, it has serial/parallel-conversion circuit 1E, parameter register 1F, and restoration circuit 1I for every port.

[0038] Serial/parallel-conversion circuit 1E is prepared in reception enabling / disable circuit 1B, and juxtaposition, receives received-data 1A regardless of enabling / disable condition of reception enabling / disable circuit 1B, changes it into parallel data from serial data, and compares with the set point of parameter register 1F. It is carried out in order to detect whether the transmitting agency address of this comparison actuation of received data corresponds with the address of the reception authorization terminal beforehand set as parameter register 1F.

[0039] Even if the receiving disable is pronounced by control signal 1C, restoration circuit 1I is a circuit which sets reception enabling / disable circuit 1B as enabling state, when coincidence detecting-signal 1H are generated from serial/parallel-conversion circuit 1E.

[0040] That is, in the configuration of this drawing 3, when a port P1 is a receiving disable, for example, received-data 1A is disregarded by control signal 1C (drawing 3 1 J), and received data are not outputted to 1D. However, also in this condition, received-data 1A is always received in serial/parallel-conversion circuit 1E, and the monitor of the that transmitting former addresses (or transmission place address etc.) is performed. The physical address of each terminal registered beforehand is set as register 1F, and is always compared with the address value of serial/parallel-conversion circuit 1E.

[0041] When both agree, even if coincidence of the address is notified to restoration circuit 1I in signal 1H and receiving disable signal 1C (here 1C2) is generated from the common control section 3, restoration circuit 1I will judge that it is data from a just terminal, and will change reception enabling / disable circuit 1B to enabling state.

[0042] In this case, since there is risk of the head of the received data of reception enabling / disable circuit 1B being cut, even if it is in a disable condition, it is desirable to adopt technique, such as to form the buffer holding received data in to reception enable / disable circuit 1B. In this case, the contents of that receive buffer will be read if a port is enabling, and if they are disables, they will not be read.

[0043] Only network access of an unjust terminal can be prevented in this configuration, without

affecting transmission and reception of other terminals other than an unjust terminal, since it is constituted so that reception actuation may be permitted when in agreement with the address information into which the transmitting agency address of the data supplied to the port where reception actuation was forbidden was registered beforehand.

[0044] Next, with reference to drawing 4, the example of construction of the network system using the network repeating installation 11 with the configuration of drawing 2 or drawing 3 is explained. In this network system, two or more network repeating installation 11 is combined in the shape of a mesh through the LAN segment, and the multi-statement of the data transfer path to the terminal on other LAN segments from the terminal on a certain LAN segment is carried out by this.

[0045] In this case, it becomes possible to usually perform enabling / disable control of a port so that the path between a certain terminals may serve as a point-to-point, to perform enabling / disable control of the port by the command according to failure generating or a traffic condition, and to perform employment of changing that path automatically or artificially.

[0046]

[Effect of the Invention] As mentioned above, according to this invention, it comes to be able to carry out enabling / disable control of each port if needed, and it becomes possible to perform prevention of the network use by the unjust terminal, a detour setup at the time of failure generating, etc.

[Translation done.]

*** NOTICES ***

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] Network repeating installation characterized by to provide the port control means which has two or more ports connected to a network, respectively, receives two or more transmitter-receivers prepared for said every port, and the command from the outside, responds to the command in the network repeating installation which interconnects a network by the data transfer between these ports, and permits / forbids transmission or reception actuation of two or more of said transmitter-receivers according to an individual for every port.

[Claim 2] In the network repeating installation which has two or more ports connected to a network, respectively, and interconnects between networks by the data transfer between these ports Two or more transmitter-receivers prepared for said every port, and the port control means which receives the command from the outside, responds to the command, and permits / forbids transmission or reception actuation of two or more of said transmitter-receivers according to an individual for every port, Network repeating installation characterized by providing a reception prohibition discharge means to cancel prohibition of reception actuation of the transmitter-receiver which compares the transmitting agency address of the data supplied to the port where reception actuation was forbidden with the address information of the terminal registered beforehand, and corresponds when in agreement.

[Claim 3] It is a network system possessing two or more network repeating installation which interconnected so that the multi-statement of the data transfer path to the terminal [terminal / on a network] on other networks could be carried out. Two or more ports where said each network repeating installation is connected to a network, Two or more transmitter-receivers prepared for said every port and the command from the outside are received. The network system characterized by providing the port control means which responds to the command, and permits / forbids transmission or reception actuation of two or more of said transmitter-receivers according to an individual for every port, and enabling it to set the data transfer path from a transmitting agency terminal to the end of a transmitting tip as arbitration.

[Translation done.]

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.